The Serials Librarian, 1993, Vol. 23, No. 3-4, p.293-296.
ISSN: 0361-526X (Print), 1541-1095 (Online)
DOI: 10.1300/J123v23n03_41
http://www.tandfonline.com/
http://www.tandfonline.com/toc/wser20/current
http://www.tandfonline.com/doi/abs/10.1300/J123v23n03_41
http://dx.doi.org/10.1300/J123v23n03_41

Auditing the Automated Serials Control System

Carol Pitts Hawks
Sandra Weaver

Workshop Leaders

David Winchester

Recorder

Carol Pitts Hawks, Head, Acquisitions Department at the Ohio State University Libraries, and Sandra Weaver, Vice-President, Innovative Interfaces, Inc., collaborated on this workshop about the auditing of an automated serials control system.

By definition an audit is a methodical examination and review of a situation or condition, concluding with a detailed report of findings. An audit trail is a fundamental component of any audit. By way of background, Hawks explained that audit trails permit an auditor to identify each step in the acquisitions process from planning of the initial order through the receipt of the material. Audit trails may be traced "backwards" by following the material back through the acquisitions process to the original purchase order. Throughout the auditing process the auditor focuses on specific and primary concerns. Are appropriate controls built into the automated system, and are these controls being used properly? Hawks reported that one of the biggest issues is who did what, and by whose authority. An auditor may address these concerns by asking specific questions. Did the appropriate person sign the voucher for payment? Did the collection manager initial the request for purchase? Did the system verify the password of the person who signed on to the system to process the order? Were passwords made available to and used by inappropriate personnel?

Automated systems have built-in checks for identifying errors. In this process the key operative word is "prevent"-to prevent errors, fraud, or waste rather than to merely detect them. Hawks explained that there are two types of controls. General control mechanisms apply to all aspects of a system, while application controls are concerned with specific computer applications and the software used to perform the functions of the system. All controls must be balanced against cost effectiveness and carefully checked for redundancy.

General control mechanisms can be divided into those controls which separate computer data processing functions, and those that control access to equipment and data files. The segregation of staff is an example of the first type. In this example the staff, who maintain and service the physical system are segregated from those staff members who might perform specific

serials tasks with the system. Limiting access to data files can be achieved by several methods. The primary and most obvious means of limiting access is through password controls. Actual physical access should be controlled by making the computers secure. The final method is by limiting the electronic access by external users of the system. This control becomes more significant as users increasingly use remote location access and as more vendors develop EDI capabilities.

In the discussion of application control mechanisms Hawks concentrated on activities and control by passwords. She presented three principal activities to be segregated: authorization, custody of assets, and accounting. These activities are translated in the acquisitions/serials system to mean purchase order preparation (authorization), receipt of material (custody), and invoice processing/payment (accounting). Passwords can be used to control many tasks in a system. They can block access completely, or can limit access to high-, medium-, or low-security files or data. Passwords can be very restrictive and allow extremely specific tasks. One password may only read data, while another may allow read and modify capabilities. Some systems may choose to separate, add, or delete data functions with unique passwords. While systems do allow for password flexibility, there are certain set conditions which govern password effectiveness. Passwords must be kept secret, not written down, and not shared with another user. The most secure passwords are those which are randomly generated. If passwords are not randomly selected, then they should be difficult to guess and be changed periodically.

A computer offers wonderful mechanisms to facilitate either the correct or incorrect recording of data and to assist in any auditing process. An audit may become a fact of life for most systems. Hawks concluded from experience that the auditing process raises important questions and accentuates areas that need attention. How long should you keep records and on what schedule should these be purged? A department head is vulnerable and it is wise to minimize the number of staff with so-called "super" passwords. Keep a watchful eye on the maintenance of paper/electronic trails in any purchase procedure. And perhaps most importantly, remember that a system cannot always detect human error.

Sandra Weaver concluded the workshop with observations from the viewpoint of an automated systems vendor. Innovative Interfaces has responded to the desires of both auditors and library staff to offer system enhancements. In discussions with auditors Weaver acknowledged that they are not always enemies. Auditors want to do things correctly; systems design should mirror this desire.

She has observed libraries which have gone through extensive audits, and she has found that auditors will listen to philosophical arguments. However, if a library has a minimal staff and an audit requires that a department have more layers of segregation of control than staff, does that library hire more staff? Everyone wants to do things correctly, but what is the price of control?

There are two different types of system audits. The first is an audit of the financial programs. This important, yet simple, audit checks that the dollars and cents add up. The basic goal is to add one and one to equal two. If a system cannot perform mathematical equations at this minimal level then it cannot hope to pass a financial audit at any basic level. Weaver acknowledged that from an auditing Standpoint a system can have problems. One example can be observed in an acquisitions/serials system when a library attempts to delete funds from the system.

She complemented Hawks' discussion of access by raising and expanding on the issue of who has access to the system and to which parts of the system. As one might expect, libraries vary widely in their response to these questions. There are many different ways by which staff and non-staff alike can have access to any system. The constant element in any access question is that it gets more complex as the system gets larger. More options equal more complicated access. As a

result, maintenance and back-ups become more complicated. With the element of access, system designers wrestle with control vs. flexibility.

Weaver raised questions specifically about the types of access. Where is the CPU located? What types of terminals are to be used and where? Is the system to offer dial-up ports? Does a single port support different types of services? How secure are technical services passwords when a system is confronted with Internet access? Can non-authorized persons get into operating systems levels? She argued that these are important yet basic questions which must be addressed.

A system needs a balance between control of access and cost effectiveness of providing that access. An audit may be a good check on procedures. Libraries are more frequently turning to the "one stop shopping" method of entering a record once and never having to touch it again; they are moving into EDI with less manual manipulation of data. Libraries seek to find systems which provide a combination of ease of use at greater speed with increased flexibility and the greatest savings in staff time. But who has control?